REMARKS

Claims 1-18 were pending at the time of the Final Office Action. In this Amendment, claims 1, 3, 10, 12 and 18 have been amended to clarify an aspect of the invention. Support is found in, for example, FIG. 7 and corresponding descriptions. Claims 1, 3-16 and 18 are currently pending for examination, of which claims 1, 7, 10 and 12 are independent. Care has been exercised not to introduce new matter.

No new issue has been introduced by the amendments to claims, since amendments to claims 1, 10 and 12 inherit subject matter of cancelled claim 2; amendment to claim 10 and amendments to claims 3 and 18 updates their dependencies.

REJECTION OF CLAIMS UNDER 35 U.S.C. §102

Claims 1, 4, 5, 7, 8 and 10-16 were rejected under 35 U.S.C 102(b) as being anticipated by Ohta et al. (US 7,158,637) herein referred to as Ohta. The rejection is respectfully traversed for the following reasons.

Amended claim 1, *inter alia*, recites "the cryptographic processing unit manages the sequence of commands executed in each cryptographic input and output process and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command," which is inherited from previous claim 2.

As admitted on page 7 of the Office Action, Ohta fails to disclose the limitations of claim 1 regarding "the cryptographic processing unit manages the sequence of commands executed in each cryptographic input and output process and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced

command." Therefore, the rejection with respect to claim 1 and claims dependent thereupon is rendered moot.

Claims 7 and 12 recite similar limitations to claim 1 respectively regarding "the cryptographic processing unit rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input and output process to which the command belongs," and "rejecting the execution of the received command when the received command has been determined to be an incorrectly sequenced command." Therefore, claims 7 and 12 and claims dependent thereupon are patentable over Ohta because Ohta fails to disclose the limitations of claims 7 and 12 as admitted by the Examiner.

Amended claim 10, in pertinent part, recites "when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input and output processes the command belongs and to manage the sequence of commands executed in each cryptographic input and output process." As disclosed in FIG. 8, by way of example of what is recited in claim 10, cryptographic input/output processing for writing license data is divided into secure commands such as the certificate output command (S102), the challenge key input command (S120), the session key preparation command (S132), the session key output command (S142), the license data input command (S158), and the license data write command (S168), thereby assigning the sequence ID to a series of cryptographic input/output processing. This makes it possible to identify to which process system a secure command belongs even when a plurality of cryptographic input/output processing are executed simultaneously. (see paragraphs [0084] of the application-as-published)

Otha, at a minimum, fails to disclose the limitations of claim 10 regarding "when the controller issues a command, the controller attaches identifying information to the command to

identify to which one of the plurality of cryptographic input and output processes the command belongs and to manage the sequence of commands executed in each cryptographic input and output process."

As anticipation under 35 U.S.C. § 102 requires that each element of the claim in issue be found, either expressly described or under principles of inherency, in a single prior art reference, *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 USPQ 781 (Fed. Cir. 1983), based on the foregoing, it is submitted that Ohta does not anticipate claims 1, 7, 10 and 12, nor claims dependent thereupon.

REJECTION OF CLAIMS UNDER 35 U.S.C. §103

Claims 2, 3, 17 and 18 were rejected under 35 U.S.C §103(a) as being unpatentable over Ohta et al. (US 7,158,637) herein referred to as Ohta as applied to claims 1, 4, 5, 7, 8 and 10-16 above, and further in view of Callum (US 6,295604) herein referred to as Callum. Claims 6 and 9 were rejected under 35 U.S.C §103(a) as being unpatentable over Ohta as applied to claims 1, 4, 5, 7, 8 and 10-17 above, and further in view of Porter et al. (U.S. Publication No. 2003/0226029, hereinafter "Porter"). The rejections are respectfully traversed for the following reasons.

The proposed combination of Ohta, Callum and Porter fails to disclose the limitations of claim 1 regarding "the cryptographic processing unit manages the sequence of commands executed in each cryptographic input and output process and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command."

While the Examiner admitted that Ohta fails to disclose the limitations of claim 1 regarding "the cryptographic processing unit manages the sequence of commands executed in each cryptographic input and output process and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command," the Examiner referred to Callum as disclosing the limitations of claim 1.

Turning to Callum, the CPP unit will set an interrupt signal of signal line 451 active and will cease operations when the following errors occurs. The errors consist of six types: (i) an incorrect header length, (ii) an incorrect data packet length, (iii) a data frame fault where the data block is not constrained in accordance with 64-bit boundaries, (iv) an initialization vector read fault where the IV data is not read before a new current data packet IV is received, (v) a write fault where a direct memory access (DMA) write occurs before the CPP unit is ready, and (vi) a read fault where a DMA read occurs from the CPP unit when no data is available. **The errors, which trigger the interruption, are directed only to errors in data frame or read and write faults, but do not care about incorrect sequence of command.** In contrast, claim 1 requires "the cryptographic processing unit" to "manage[s] the sequence of commands executed in each cryptographic input and output process," and to "reject[s] the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command." As disclosed in FIG. 7, by way of example of what is recited in claim 1, the control unit 222 checks the process status of the process system to which the secure command belongs in order to determine whether the secure command is to be executed. If the immediately preceding command of the process system has been successfully completed and the received command is a correctly sequenced command, the control unit 222 permits the command to be executed. If the immediately preceding command of the process system is being executed or aborted or the

received command is an incorrectly sequenced command, the control unit 222 rejects the execution of the command. This makes it possible to provide further improved security measures against unauthorized access.

In addition, Porter, which was cited for the normal data storing unit and the confidential data storing unit, fails to cure deficiencies of Ohta and Callum.

Accordingly, as each and every limitation must be disclosed or suggested by the cited prior art references in order to establish a *prima facie* case of obviousness (*see*, M.P.E.P. § 2143.03) and for at least the foregoing reasons the proposed combination of Ohta, Callum and Porter fails to do so, it is respectfully submitted that claim 1 and claims dependent thereupon are patentable over the combination of Ohta, Callum and Porter.

As addressed above, claims 7 and 12 recite the substantially similar limitations to claim 1. Claims 7 and 12 and claims dependent thereupon are patentable over the proposed combination of Ohta, Callum and Porter for the same reasons as claim 1.

Conclusion

In view of the above amendments and remarks, Applicants submit that this application should be allowed and the case passed to issue. If there are any questions regarding this Amendment or the application in general, a telephone call to the undersigned would be appreciated to expedite the prosecution of the application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Hosang Lee
Registration No. L00,295

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 SAB/HL:cac
Facsimile: 202.756.8087
Date: October 20, 2008

Please recognize our Customer No. 20277 as our correspondence address.

WDC99 1639522-1.065933.0083